WispSwap: a Decentralized Exchange and Prediction Market on Sui blockchain

Alex Xu
alex@wispswap.io
WispSwap Labs

Matthew Pei
matthew@wispswap.io
WispSwap Labs

***Abstract*—The DeFi space has experienced exponential growth in recent years, with DEXs at the forefront of this innovation. However, the current landscape of AMM DEXs still presents challenges, such as substantial impermanent loss, limited functionalities, and scalability issues. WispSwap is a novel AMM DEX on Sui blockchain, designed to contribute to the ever-evolving DeFi space. The platform's architecture has been thoughtfully designed to enhance users' experience and provide advanced trading capabilities. This whitepaper aims to provide a conceptual framework of AMM DEXs and Decentralized Prediction Market (DPM), making it an essential read for anyone interested in DeFi. It also discusses the reason behind launching WispSwap on Sui blockchain, along with a comprehensive overview of the platform. Moreover, the paper highlights the distinctive features of WispSwap, including its A-CLMM mechanism and cross-chain prediction protocol, and its competitive edge over other DeFi protocols in the market.**

***Index Terms*—A-CLMM, cross-chain prediction, DPM, Sui Blockchain, WispSwap**

I. Introduction

A. Background

The DeFi ecosystem has undergone significant evolution and has gained traction due to its potential to disrupt traditional financial systems [1]. The introduction of the Ethereum Virtual Machine [2] (EVM) allowed software engineers to build self-executing computer programs (called smart contracts), which facilitated the creation of Decentralized Applications (DApps). One of the earliest DApps built on EVM is a DEX that enabled peer-to-peer trading of assets without the need for a centralized entity.

While DEXs have provided an alternative to centralized exchanges' custodial, non-transparent, and self-serving models, they have been not without flaws [3]. DEXs with a high total value locked (TVL) were presumed to be reliable and trustworthy, which led to a significant increase in the number of traders and trading volumes. To achieve comparable status, rather than focusing on maximizing the utility of existing liquidity through technical architecture design, every DEX redirected its main focus to acquiring liquidity. DEX projects began offering liquidity rewards that exceeded the actual value generated from trading transactions, resulting in a race to the bottom for all stakeholders In the midst of this turmoil, the concept of concentrated liquidity emerged as a potential solution.

The concentrated liquidity market maker (CLMM) model distributes liquidity across narrow price ranges rather than wide price ranges, which allows liquidity providers to construct custom price curves that align with their preferences. This innovation in AMMs enhances the capital efficiency of DEXs and enables them to process more orders with less liquidity.

Despite the growth of DEX platforms in recent years, the trading volume on CEXs still dominates the crypto market. As of April 2023, According to CoinGecko [4], the 24-hour trading volume of the top 10 CEXs ranges from $2.5 billion to $27 billion, while the top 10 DEXs have a trading volume between $200 million to $3.5 billion. This trend can be attributed to several factors, including lower liquidity, slower transaction speeds, and higher fees on DEXs, as well as the lack of mainstream adoption of cryptocurrencies. Furthermore, the lack of advanced trading capabilities in DEXs has also contributed to this gap. The declining activity of DEXs is further exacerbated by the rise of Maximal Extractable Value [5] (MEV) attacks in decentralized venues which have further restricted liquidity from flowing into DeFi. Therefore, it is crucial for DEX infrastructure to evolve to address these issues and provide a better trading experience.

B. Overview of WispSwap

WispSwap is a novel AMM DEX built on Sui blockchain, one of the most advanced Layer 1 (L1) blockchain technologies available, with the aim of contributing to the continuously evolving DeFi space. The platform's offerings include lending, farming, staking, prediction markets and launchpad services, making it a comprehensive DeFi solution for users.

The Asymmetric Concentrated Liquidity Market Maker (A-CLMM) mechanism was developed by leveraging the foundational innovation of Uniswap V3's [6] CLMM. Compared with the traditional CLMM, A-CLMM offers advanced trading features such as the ability for liquidity providers to select two different ranges for two directions of the swap. This feature provides more flexibility in adjusting liquidity for different trading pairs, allowing liquidity providers to optimize their returns while still providing impermanent loss protection and capital efficiency improvements. In addition, Wisp-Prediction, our Decentralized Prediction Market [7] (DPM), is the first-of-its-kind product built on Sui blockchain. It enables users to earn rewards by predicting on crypto prices and real-world events and earn rewards. With our (Real-Time Gross Settlement [8]) RTGS-type system, users can participate in prediction markets across various chains, thereby providing

a deeper prediction pool. By combining the technology advancement of Sui blockchain [9] with WispSwap's robust architecture, the platform's goal is to meet or surpass the offerings of comparable protocols in terms of features and functionality.

II. Conceptual Framework

A. Automated Market Maker Decentralized Exchange

This section presents Automated Market Maker Decentralized Exchange (AMM DEX)'s fundamental concepts, main components, including different actors, as well as their generalized mechanism and economics

1) Core actor:

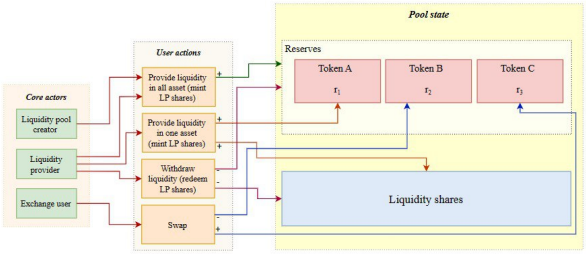

Fig. 1. AMM DEX Core Actors and Dynamics

a) Liquidity Provider (LP): A pool creator is the first to supply crypto assets into a pool. Other LPs can add more crypto assets to the pool to increase its reserve. As compensation for liquidity contribution, LPs are rewarded with a proportional allocation of pool shares based on their contributed assets relative to the entire pool's reserve. In addition, they receive transaction fees paid by exchange users. However, LPs' primary concern is the possibility of experiencing impermanent loss.

b) Exchange user: Traders submit exchange orders to liquidity pools with input and output assets, and the smart contract calculates and executes the exchange rate based on a conservation function. Each trade incurs a fee to compensate liquidity providers for their liquidity contribution.

c) Arbitragers: Arbitrageurs are exchange users who seek profit by comparing asset prices in various markets and executing trades to capitalize on closing price gaps. Their actions facilitate "price discovery" across a variety of exchanges. One strategy that certain AMM protocols employ to mitigate impermanent loss involves intentionally facilitating arbitrary activities.

For instance, the DODO DEX [10] mechanism leverages external market data as a significant factor in determining the exchange rate, thereby presenting an arbitrage opportunity in the pool. By utilizing price alignment through arbitrage, the reserve ratio is pulled back to its equilibrium state set by the LP, effectively eliminating any divergence loss. This feature distinguishes DODO from other AMMs, and its pricing algorithm is referred to as a "proactive market maker," or PMM.

2) Fundamental AMM dynamics:

a) Conservation function: An AMM's functionality is underpinned by a conservation function that reflects a desired invariant property of the system. For instance, Uniswap V2's constant product function resolves the trading dynamics between assets in the pool by conserving the product of value-weighted quantities of both assets in the protocol. This means that any trade made in the pool must maintain the equality between the removed and added values of the assets. The weight-preserving feature exemplifies a desired invariant property that is fostered by Uniswap's design. Another example of an invariant property in an AMM is Uniswap V3's [6] concentrated liquidity market maker (CLMM [11]). In CLMM, liquidity providers can concentrate their liquidity around a specific price range to optimize their capital efficiency. The invariant property is the conservation of the constant product of the liquidity in each price range, ensuring that the total liquidity and price range coverage are constant, and that the liquidity is always available for trades within the specified price range.

b) Mechanisms: AMMs typically have two types of interaction mechanisms: asset swapping and liquidity provision/withdrawal. The interaction mechanisms used in AMMs must be designed in a way that preserves desired invariant properties. As a result, the class of acceptable mechanisms is limited to those that preserve the conservation function, if one is defined, or maintain the defined properties in the absence of a conservation function.

3) Fundamental AMM economics:

a) Rewards:

- *Liquidity reward* Liquidity providers are incentivized to supply assets to a liquidity pool. However, they also incur opportunity costs associated with funds being locked in the pool. In exchange for this contribution, liquidity providers receive a portion of the trading fees paid by exchange users.
- *Staking reward* In addition to transaction fees as a liquidity reward, liquidity providers are often offered a staking reward, which incentivizes them to hold and stake specific tokens as part of an initial incentive program from the token protocol. Staking rewards offer a way for liquidity providers to earn additional tokens by staking them in the exchange's liquidity pools. These rewards are typically distributed in proportion to the amount of liquidity a provider contributes to the pool. The primary goal of staking rewards in AMM exchanges is to encourage token holding while also facilitating token liquidity on exchanges. Staking rewards are a popular incentive mechanism used in decentralized finance (DeFi) protocols and have become an important part of the broader ecosystem.
- *Governance right* AMMs can encourage liquidity provision and/or swapping by offering participants governance rights in the form of protocol tokens, which are termed "governance tokens". These tokens not only provide a means of incentivizing participants, but also give them a voice in the governance of the protocol. By doing so,

AMMs can cultivate a sense of community ownership and engagement. At present, governance issues related to protocol treasury management are typically proposed and deliberated on governance portals such as Snapshot [12], Gnosis [13], Aragon [14], and MolochDAO [15], where protocol tokens are utilized as voting ballots for proposals

- *Bug bounty reward* Similar to other protocols constructed on an open and decentralized blockchain network, AMM DEXes are susceptible to security vulnerabilities. In addition to conducting code audits, it is a standard practice for protocol foundations to have the code inspected by a wider developer community and offer monetary incentives to those who identify and/or fix protocol's bugs.

b) Explicit costs:

- *Gas fee* As users engage in token exchanges with the liquidity pool, they are required to compensate the LPs for providing the assets and covering Impermanent losses (refer to II-A3b). These swap fees are charged on each exchange trade and then distributed to liquidity pool shareholders, with a portion potentially allocated to the AMM foundation to support protocol development.
- *Swap fee* Every interaction with the protocol requires an on-chain transaction and is subject to a gas fee that the user initiating the transaction must pay. This fee compensates validators for their work in processing and verifying the transaction. Interacting with more complex protocols or executing transactions during times of high network congestion may result in higher gas fees.
- *Liquidity withdrawal penalty*
  When a LP withdraws liquidity from an AMM DEX, it alters the shape of the conservation function, which negatively affects the pool's usability by elevating slippage. To mitigate this issue, some AMM DEXs impose a liquidity withdrawal penalty.

c) Implicit costs:

- *Slippage* Slippage refers to the difference between the spot price and the realized price of a trade. Instead of matching buy and sell orders, Automated Market Makers (AMMs) determine exchange rates on a continuous curve, which leads to slippage. This slippage is dependent on the trade size in relation to the pool size and the design of the conservation function. For smaller liquidity pools, every trade significantly impacts the relative quantities of assets, leading to higher slippage. The spot price approaches the realized price for infinitesimally small trades, but deviates more for larger trade sizes.
- *Impermanent loss* When LPs supply assets to a protocol, they are exposed to volatility risk, in addition to the loss of time value of locked funds. The asset composition of a pool is automatically updated with every swap, changing the asset prices implied by the conservation function of the pool (Refer). This change in value of the entire pool, as opposed to holding the assets outside of an AMM pool, results in less value with price movement, known as "impermanent loss" or "divergence loss". This loss can be deemed "impermanent" since the depreciation of the pool value continuously disappears and reappears as asset prices move back and forth, and is only realized when assets are removed from the pool. Effective AMMs ensure that LPs are adequately compensated for the divergence loss by charging appropriate swap fees.

B. Decentralized Prediction Market

A decentralized prediction market (DPM) is a permissionless platform that provides users with the ability to make predictions on the potential outcomes of future events, using cryptocurrencies or other digital assets. This section aims to explicate the fundamental components that constitute a DPM, including the various actors involved in the system and the practical life cycle of a DPM.

1) Core Actor:

a) Market Creator: The market creator takes on the responsibility of creating and structuring the market's questioning and resolution regulations. Additionally, they have the option to establish a fee structure to earn a percentage of market share settlements during trading or market resolution. To promote the market and attract more traders, the creator can also set up an affiliate fee, which incentivizes affiliates to promote the market and collect fees every time someone follows their link and trades in the market. Moreover, establishing initial market liquidity by adding buy and sell offers with sizable volumes on each side is another way to ensure the market's attractiveness to users.

b) Market Participant: Market Participants are individuals who participate in the market by making predictions on the outcome of a specific event. As a result of their participation, Market Participants incur costs, which are paid to the Market Creator and the DPM platform. These costs may take the form of trading fees or other transactional costs, which are used to maintain the integrity and security of the platform. In addition, Market Participants may also incur costs associated with market outcomes that differ from their predicted outcome. These costs are distributed among all participants who held positions in the market and are calculated based on the outcome of the event. Therefore, it is important for Market Participants to carefully consider the risks and potential costs associated with their participation in decentralized prediction markets.

2) Life cycle of a DPM: The cycle starts by setting up a market and establishing the market's question and resolution rules. After the market is established, users may participate by entering a prediction position. Once the market's closing date arrives, an oracle will identify the potential winning outcome and provide the result. Afterward, funds will be distributed to those who hold the winning outcome tokens. We will delve into each stage of the process in more detail.

a) Market creation phase: To create a market, the creator must ensure they have the necessary cryptocurrency funds in their wallet. When creating a market, the creator will be required to pay a validity fee and a transaction fee. The validity fee is designed to prevent poorly defined markets, and the

creator can collect it back if the market resolves to anything other than invalid. The transaction fee is nonrefundable and is used to establish the market on a blockchain. To create a market, the first step is to define a question with all possible outcomes. Typically, there are three market types: Binary (Yes/No or Up/Down), Multiple Choice, and Scalar. After setting up the question, the market creator needs to determine the resolution information, including the designated reporter and resolution rules. If the designated reporter fails to report, the market enters the Open Reporting phase. Users can dispute the report before the market resolves.

b) Prediction phase: Once the prediction market is created, users can participate by entering a prediction position, where they bet a certain amount of money on the outcome they believe will occur. The amount of money wagered on a specific position determines the share of that position's pool, which is used to calculate the reward if that position becomes the winning outcome after the market ends. The larger the size of a user's position, the more significant their share of the pool, and the larger their potential reward if their position turns out to be the winning one after the market ends. Thus, users have an incentive to make informed predictions based on available information to potentially earn a reward.

c) Settlement phase: The reporting phase is initiated when a prediction market reaches its reporting start date. The primary objective of this phase is to establish consensus among market participants on the final outcome, resulting in payouts for the winners and market resolution. If available, an oracle can be used to determine the outcome. After the final outcome is determined, the size of users' positions in the winning position pool is used to calculate the payout sent to all users holding shares in these events. The payout values are organized in a matrix format that includes the events in columns and the share owners' addresses in rows. Upon completion of the payout matrix, the market broadcasts it to the DPM system. Once incorporated into a block and added to the blockchain, the payouts appear in the recipients' accounts.

III. SUI BLOCKCHAIN: FACILITATING WISPSWAP'S NOVEL DEFI SOLUTIONS

A. Overview of Sui Blockchain Technology

Sui blockchain [9] boasts several unique features that distinguish it from traditional blockchains. First, it scales horizontally, allowing network capacity to grow in proportion to validator processing power. This prevents rigid bottlenecks and results in low gas fees even during high network traffic.

Second, Sui uses a multi-lane approach to transaction validation, which allows independent transaction flows to progress without impediment from others. This Byzantine-resistant process ensures transactions are executed and signed correctly and guarantees finality

Third, Sui employs Move smart contracts to power its applications. Sui Move is a dialect of the Move programming language initially developed at Facebook for writing high security smart contracts. This design prevents common vulnerabilities such as reentrancy and poison tokens.

Fourth, on-chain assets in Sui are represented as objects and owned by users. This ensures secure ownership and prevents malicious manipulation.

Finally, Sui's programmable transaction enables the ability to call multiple functions in multiple contracts in one transaction, allowing for more efficient batching.

In comparison, traditional blockchains have limited scalability due to their rigid structure and limited throughput. Transaction validation is often sequential and can be slow, leading to high fees and poor user experience. Smart contracts are often developed in languages not specifically designed for blockchain, leading to vulnerabilities and hacks. On-chain assets are just records on a smart contract, leaving them vulnerable to manipulation. Traditional blockchains also have limited ability to batch transactions efficiently.

B. Rationale for WispSwap's decision to launch on Sui Blockchain

After conducting a thorough analysis, it is our belief that the DeFi market will experience a resurgence in mid-2023. As emerging layer 1 blockchains are expected to play a pivotal role in the DeFi market, we posit that Sui blockchain possesses the potential to become a major player in this space.

Our selection of Sui as the debut mainnet for WispSwap followed a comprehensive evaluation of the underlying technology of several layer 1 blockchains. Through this evaluation, we determined that Sui blockchain's features, including high scalability, high transaction per second (TPS), and low gas fees, make it an ideal fit for our decentralized exchange (DEX) platform.

Additionally, Sui's Object model and Move smart contract technology enhance the security of Wispswap, allowing for greater control and ownership over on-chain assets while preventing common vulnerabilities that have been exploited on other blockchain platforms. Move smart contract programming language is designed to prevent vulnerabilities such as reentrancy, poison tokens, and spoofed token approvals that have been exploited in other blockchain platforms, leading to significant financial losses.

The ability to batch transactions on the Sui blockchain is another key feature that Wispswap finds advantageous. This capability enables complex use cases and the ability to maximize profit, making it easier for Wispswap to execute trades efficiently and quickly. The strong management and governance team behind the Sui blockchain was also a factor that influenced our decision. We believe that Sui has the potential to become a leading blockchain platform for DeFi applications due to its strong team and clear roadmap.

Finally, during the time we did our research, we did not come across any other DeFi protocols being developed on Sui blockchain that offer the Asymmetric Liquidity Market Maker (A-CLMM) and Decentralized Prediction Market (DPM) features. This offering sets WispSwap apart from other protocols on Sui and provides additional benefits to users, giving WispSwap a competitive edge in the DeFi market.

IV. WispSwap's Technological Advancements

A. WispSwap's A-CLMM model

1) Concentrated Liquidity:

a) Framework: Uniswap V3 [6] introduced the concept of Concentrated Liquidity Market Maker (CLMM) as a solution to address the limitations posed by the Constant Product Market Maker (CPM) model used in Uniswap V2 [16]. In contrast to the spread-out liquidity across a price curve ranging from 0 to infinity in CPM, CLMM offers LPs the ability to concentrate their capital within customized price ranges, resulting in increased capital efficiency and lower price risk for LPs. In the CPM model, LPs earn fees on only a small portion of their capital, which may not sufficiently compensate for the price risk associated with holding large inventories in both tokens, resulting in "impermanent loss." Moreover, traders may face high degrees of slippage as liquidity is thinly spread across all price ranges. With the CLMM model, LPs can construct customizable price curves that reflect their personal preferences while providing greater liquidity at desired prices.

In addition, LPs can combine any number of distinct concentrated positions within a single pool, as shown in Figure 2. By doing so, an LP can approximate the shape of any automated market maker or active order book. Users trade against the combined liquidity of all individual curves with no gas cost increase per liquidity provider. Trading fees collected at a given price range are split pro-rata by LPs proportional to the amount of liquidity they contributed to that range. By concentrating their liquidity, LPs can provide the same liquidity depth as Uniswap V2 within specified price ranges while putting far less capital at risk. The capital saved can be held externally, invested in different assets, deposited elsewhere in DeFi, or used to increase exposure within the specified price range to earn more trading fees.

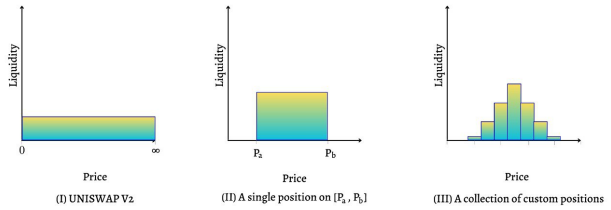

Fig. 2. Liquidity distribution comparison

b) Mathematical equations: The conservation function of a Concentrated Liquidity Market Maker (CLMM) pool is the aggregate of all individual LPs' conservation functions, which depend on the price range selected by each LP for their liquidity provision.

Suppose an LP supplies: A1 token T_1 and A2 token T_2 , with the restriction that his liquidity is only provided for users swapping within a specific range of exchange rates: $\left(\frac{p}{(1+r_1)}, p\,(1+r_1)\right)$ where $r_1 > 0$ and initial exchanges rate is $p = \frac{A_1}{A_2}$, the conservation function will be:

$$\left(a_1 + \frac{A_1}{\sqrt{1+r_1}-1}\right)\left(a_2 + \frac{A_2}{\sqrt{1+r_1}-1}\right) = \frac{(1+r_1)A_1A_2}{(\sqrt{1+r_1}-1)^2}$$

The exchanges rate can thus be calculated as:

$$E_{1,2} = \left(a_1 + \frac{A_1}{\sqrt{1+r}-1}\right) / \left(a_2 + \frac{A_2}{\sqrt{1+r}-1}\right)$$

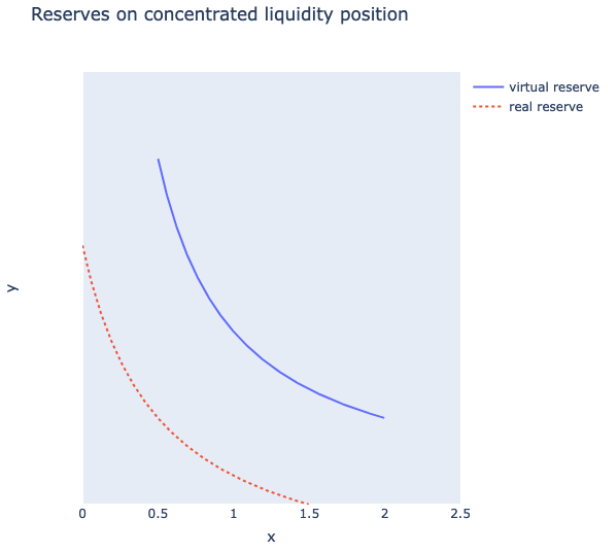

Fig. 3. Reserves in Concentrated Liquidity

B. WispSwap DEX's design

a) Framework: The Asymmetric Concentrated Liquidity Market Maker (A-CLMM) is an advanced mechanism developed for WispSwap DEX that leverages the foundational concept of Uniswap V3's [6] CLMM. The A-CLMM model improves upon the conventional CLMM by allowing liquidity providers to select two distinct price wf swap, as opposed to one range for both directions. With CLMM, liquidity providers are limited to the option of concentrating their liquidity on both sides of the swap, thereby limiting their ability to fully utilize their capital. In contrast, A-CLMM enables liquidity providers to optimize their capital allocation in either the buy or the sell direction, or even in both directions simultaneously, thereby offering greater flexibility and the potential for higher capital efficiency and better risk management. Additionally, the use of asymmetric ranges in A-CLMM allows for greater concentration of capital at desired prices and directions, which can improve the user experience by reducing slippage and enhancing execution prices.

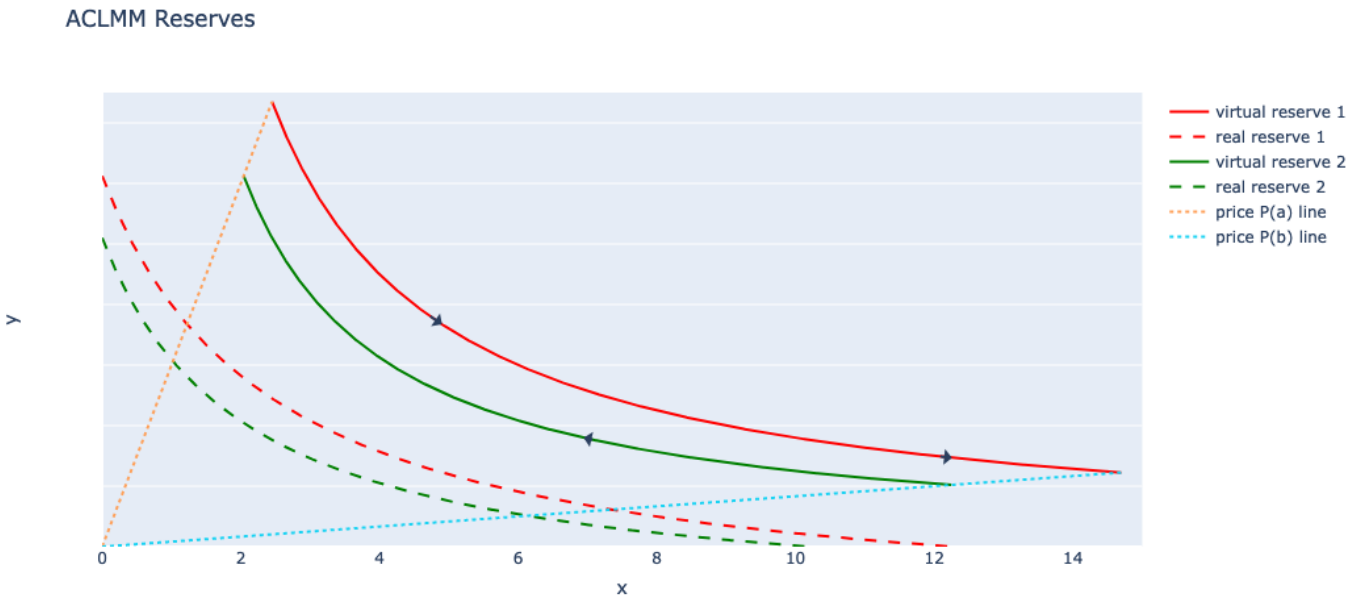

Fig. 4. A-CLMM bonding curves

b) Mathematical equations: Asymmetric Concentrated Market Maker (A-CLMM) pools have conservation functions that follow the same form for both buy and sell directions. However, A-CLMM pools have two separate bonding curves for these two directions of the swap.

Suppose an LP supplies: $A1$ token T_1 and $A2$ token T_2. The initial exchange rate is $p = \frac{T_1}{T_2}$, where $a > 0$, with the restriction that its liquidity is only provided for users swapping within a specific range of exchange rates: $\left(\frac{p}{(1+r_1)}, p\,(1+r_1)\right)$ when exchanges rate going up, this mean:

$$\Delta E_{1,2} = E_{1,2}^{trx+1} - E_{1,2}^{trx} > 0$$

An LP also provides liquidity on opposite ranges, on the same initial price with the same provision strategy: A_3 token T_1 and A_4 token T_2 at initial price $p = \frac{T_1}{T_2}$, with the restriction that its liquidity is only provided for users swapping within a specific range of exchange rates $\left(\frac{p}{(1+r_2)}, p\,(1+r_2)\right)$ where $r_2 > 0$ when exchanges rate going down, this mean:

$$\Delta E_{1,2} = E_{1,2}^{trx+1} - E_{1,2}^{trx} < 0$$

So the final conservation function will be a polynomial equation:

$$\left(a_1 + \frac{A_1}{\sqrt{1+r_1}-1}\right)\left(a_2 + \frac{A_2}{\sqrt{1+r_1}-1}\right) = \frac{(1+r_1)A_1A_2}{(\sqrt{1+r_1}-1)^2}$$

if $\Delta E_{1,2} > 0$

$$\left(a_1 + \frac{A_3}{\sqrt{1+r_2}-1}\right)\left(a_2 + \frac{A_4}{\sqrt{1+r_2}-1}\right) = \frac{(1+r_2)A_3A_4}{(\sqrt{1+r_2}-1)^2}$$

if $\Delta E_{1,2} < 0$

Exchanges rate would be:

$$E_{1,2} = \left(a_1 + \frac{A_1}{\sqrt{1+r_1}-1}\right) / \left(a_2 + \frac{A_2}{\sqrt{1+r_1}-1}\right)$$

if $\Delta E_{1,2} > 0$

$$E_{1,2} = \left(a_1 + \frac{A_3}{\sqrt{1+r_2}-1}\right) / \left(a_2 + \frac{A_4}{\sqrt{1+r_2}-1}\right)$$

if $\Delta E_{1,2} < 0$

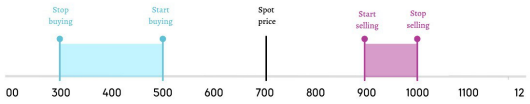

Fig. 5. Asymmetric Liquidity

c) Liquidity Provision Strategies: With these mechanisms, we offer different liquidity provision strategies for our users to choose from. These include:

- **No Liquidity Provision**: No liquidity is deposited into any pool and the portfolio is equally allocated between two tokens.

- **Passive Liquidity - Uniswap v2**: Liquidity is evenly distributed across the complete price range, similar to Uniswap v2.
- **Fixed Single Interval - Fixed**(a): Liquidity is provided to a symmetric interval around the current price, and this interval is never adjusted. Users can choose the parameter 'a' to determine the percentage interval around the current price. Resetting Single Interval - Reset(a, r): This strategy provides liquidity to the interval around the current price, with a resetting interval chosen as well. When the price moves outside the resetting interval, the liquidity position is adjusted by resetting both intervals around the current price. Users can choose the parameters 'a' and 'r' to determine the size of the intervals.
- **Fixed Dual Interval - Fixed**(a, b): This strategy involves providing liquidity to two symmetric intervals around the current price, each with a width defined by the parameters a and b. More specifically, the intervals $(p(1+a)-1, p(1+a))$ and $(p(1-b), b(1-b)+1)$ are chosen, where p is the current price. This strategy provides more liquidity than the Fixed Single Interval strategy and allows for more price movement before the liquidity position needs to be adjusted.
- **Resetting Dual Interval - Reset**(a, b, r): This strategy is similar to the Resetting Single Interval strategy, but instead of a single interval, liquidity is provided to two symmetric intervals around the current price, each with a width defined by the parameters a and b. Additionally, a resetting interval with a width defined by the parameter r is chosen. As soon as the price moves outside the resetting interval, the liquidity position is adjusted by resetting both the liquidity intervals and the resetting interval around the current price. This strategy provides more liquidity than the Resetting Single Interval strategy and allows for more price movement before the liquidity position needs to be adjusted.

C. Wisp-prediction

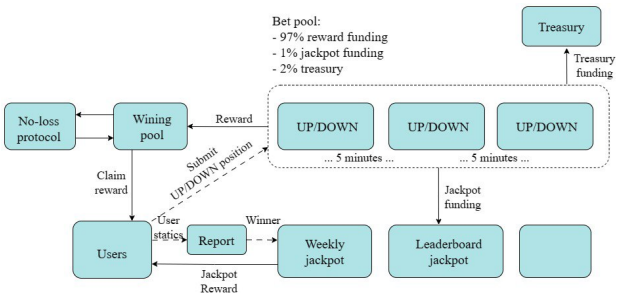

Fig. 6. Wisp-prediction Architecture

Wisp-Prediction, an implementation of Decentralized Prediction Market (DPM) on Sui blockchain, is the first of its kind on the network. In Wisp-Prediction V1, a Binary Options DPM was incorporated due to its simplicity and user-friendliness. Nevertheless, there are plans to expand Wisp-Prediction in the future by adding additional markets for users to predict on. Users will be able to bet on real-world events, including but not limited to sports and political events. Furthermore, a cross-chain prediction protocol has been designed by the WispSwap team, which will be deployed on the Sui blockchain after the mainnet launch.

1) Decentralized Prediction Market:

a) Technical architecture: In Wisp-Prediction V1, users can engage in speculation on cryptocurrency prices. New rounds of prediction are available every 5 minutes, with users able to choose to submit either an Up or Down position on the crypto price. The prediction market's Lock price and End price for each round are updated at regular intervals through the use of the Switchboard Price Oracle. This Price Oracle is integrated into the smart contract to set the prices that determine the winning positions of users. Wisp-Prediction also features a Jackpot feature, which incentivizes user engagement with the platform by distributing the jackpot to those who qualify under certain criteria, such as the highest losing streak or the largest number of bets placed, or through a random selection process. Additionally, a deflationary mechanism for the WISP token is implemented, where a small portion of the pot is allocated to the treasury for the purpose of buyback and burning of WISP tokens.

b) Mathematic Equations: A prediction market is created with two probable outcomes defined as O_1 and O_2. Assumming that there are: n players bet on O_1 and m players bet on O_2, the i^{th} players bet B_0^i on outcome O After the event happened, the total amount in the pool will be:

$$TotalPrize = \sum_{i=1}^{n} B_{o_1}^i + \sum_{i=1}^{m} B_{o_2}^i$$

- Assume that O_1 is the accurate outcome, the i^{th} winner will receive the amount of winning token R^i :

$$R^i = \frac{B_{O_1}^i}{\sum_{i=1}^{n} B_{O_1}^i} \left(\sum_{i=1}^{n} B_{O_1}^i + \sum_{i=1}^{m} B_{O_2}^i \right)$$

2) Cross-chain prediction protocol:

a) Technical architecture: RTGS (Real Time Gross Settlement) is a payment system used for immediate settlement of large-value transactions. Transactions are processed in real-time, reducing counterparty risk and increasing efficiency. Our team has designed a RTGS-type system to enable users to participate in prediction markets across various chains. When a user submits a prediction position in another L1 blockchain, a message containing information on the positions will be transmitted to the staging pool in Sui. These cross-chain prediction messages will then be combined with Sui prediction information on this staging area, enabling the platform to pre-calculate the payout amount and display accurate data to users. After each round, prefunding liquidity pools on different L1s are utilized to distribute winning rewards to cross-chain winners. At specified intervals, the contracts on the other chains transfer real tokens to these prefunding liquidity pools through our bridge infrastructure, guaranteeing that these pools

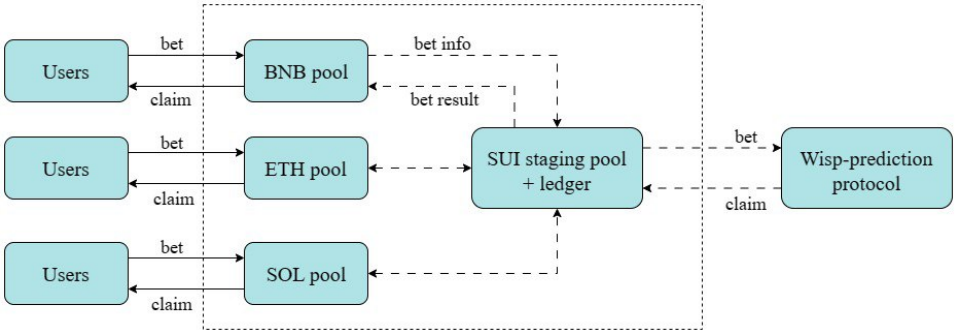

Fig. 7. Cross-chain prediction protocol architecture

have sufficient token amounts and ensuring that users receive their payouts in a timely and accurate manner.

b) Benefits: Our Cross-chain prediction protocol provides two significant benefits. First, by aggregating liquidity from multiple chains, we are able to balance both sides of the binary prediction game and create a more efficient market. The greater the liquidity we can gather, the more opportunities there are for users to engage in prediction markets with fair and accurate pricing. Secondly, this approach facilitates the flow of funds not only to Sui but also to other chains, thereby strengthening the overall ecosystem. By encouraging cross-chain liquidity, we can create a more interconnected and robust prediction market that benefits all participants.

V. Conclusion

In this paper, we have presented a comprehensive conceptual framework for AMM DEXs and Decentralized Prediction Market (DPM), providing essential insights for those interested in DeFi. Moreover, the paper delves into WispSwap, a novel AMM protocol on the Sui blockchain, which aims to contribute to the ongoing evolution of DeFi. WispSwap's unique features include its Asymmetric Liquidity Market Maker (A-CLMM), the first implementation of Decentralized Prediction Market (DPM) on Sui blockchain called Wisp-Prediction, and a Cross-chain Prediction Protocol. These features give WispSwap a competitive edge over other DeFi protocols in the market. The research presented in this paper lays the foundation for further exploration and development of AMM DEXs and DPMs on blockchain networks.

References

[1] M. Swan, *The Definitive Guide to DeFi: How Decentralized Finance is Disrupting the Financial System*. Apress, 2020.

[2] V. Buterin, "Ethereum white paper," 2013.

[3] T. Elbahrawy, A. E. El-Esawi, M. Elsherif, and A. Helmy, "Decentralized vs centralized exchanges: A comparative study," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2019, pp. 139–148.

[4] CoinGecko, "Coingecko," 2023. [Online]. Available: https://www.coingecko.com/en/exchanges

[5] P. Daian, S. Goldfeder, A. Kell, I. Bentov, and A. Juels, "Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges," in *Proceedings of the 27th USENIX Security Symposium*, 2020, pp. 2231–2248. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/daian

[6] H. Adams and N. Zinsmeister, "Uniswap v3 whitepaper," 2021. [Online]. Available: https://uniswap.org/whitepaper-v3.pdf

[7] J. Peterson, J. Krug, M. Zoltu, A. K. Williams, and S. Alexander, "Augur: a decentralized oracle and prediction market platform," 2018. [Online]. Available: http://rgdoi.net/10.13140/2.1.1431.4563

[8] C. M. Kahn and W. Roberds, "Real-time gross settlement and the costs of immediacy," *Journal of Monetary Economics*, vol. 47, no. 2, pp. 299–319, 2001. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0304393201000472

[9] M. Labs, "Sui blockchain whitepaper," 2022. [Online]. Available: https://github.com/MystenLabs/sui/blob/main/doc/paper/sui.pdf

[10] DODO, "Dodo whitepaper," 2020. [Online]. Available: https://dodoex.github.io/docs/docs/

[11] R. Fritsch, "Concentrated liquidity in automated market makers," in *Proceedings of the 2021 ACM CCS Workshop on Decentralized Finance and Security*, ser. DeFi '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 15–20. [Online]. Available: https://doi.org/10.1145/3464967.3488590

[12] "*Snapshot*," https://snapshot.org/, accessed: 2022-03-30.

[13] "*Gnosis*," https://www.gnosis.io/, accessed: 2022-03-30.

[14] "*Aragon*," https://aragon.org/, accessed: 2022-03-30.

[15] MolochDAO, "Molochdao," 2019. [Online]. Available: https://molochdao.com/

[16] H. Adams, "Uniswap v2 whitepaper," 2020. [Online]. Available: https://uniswap.org/whitepaper.pdf